NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Risk Management Framework (RMF) Small Enterprise Quick Start Guide

A Comprehensive, Flexible, Risk-Based Approach to Managing Information Security and Privacy Risk

NIST Special Publication
NIST SP 1314
https://doi.org/10.6028/NIST.SP.1314
July 2024

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

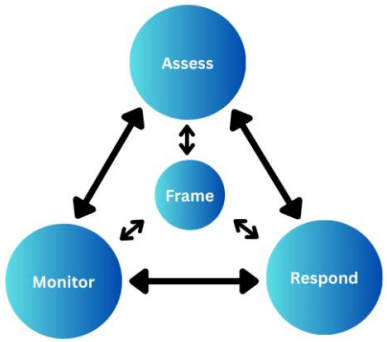
Overview

Purpose of this Small Enterprise Quick Start Guide

For organizations of all sizes, managing risk (including information security[1] and privacy risk) is critical for organizational resilience. This guide is designed to help small, under-resourced entities understand the value and core components of the NIST Risk Management Framework (RMF)[2] and provide a starting point for designing and implementing an information security and privacy risk management program. *This document is not intended to replace the RMF; it is intended to be an introductory guide to help organizations get started*.

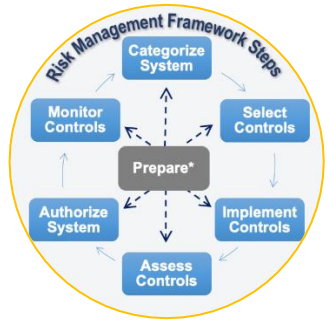
Risk Management Fundamentals

Before we explore the RMF in detail, let's take a moment to understand risk management broadly. Risk management is a comprehensive process that enables organizations to:



- **Frame Risk**: Establish a risk context by providing a common perspective on how organizations manage risk. A key output is the risk management strategy that addresses risk tolerance, assumptions and constraints, and how the organization intends to assess, respond to, and monitor risk.
- **Assess Risk**: Identify, prioritize, and estimate risk impacts to the organization, operations, and mission/business. Learn more about Conducting Risk Assessments in SP 800-30.
- **Respond to Risk**: Identify, evaluate, decide on, and implement appropriate courses of action to accept, avoid, mitigate, share, or transfer risk.
- **Monitor Risk**: Verify planned risk response measures are implemented, determine the ongoing effectiveness of the risk responses, and continuously monitor risk.

The NIST RMF



The RMF provides a **comprehensive, flexible, repeatable, and measurable** seven-step process that organizations can use to manage their unique information security and privacy risks. The RMF can be applied to new and existing systems, any type of system or technology (e.g., Internet of Things, control systems), and within any type of organization regardless of size or sector.

[1] Information security, often used interchangeably with the term "cybersecurity," is the protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction. See full definition.

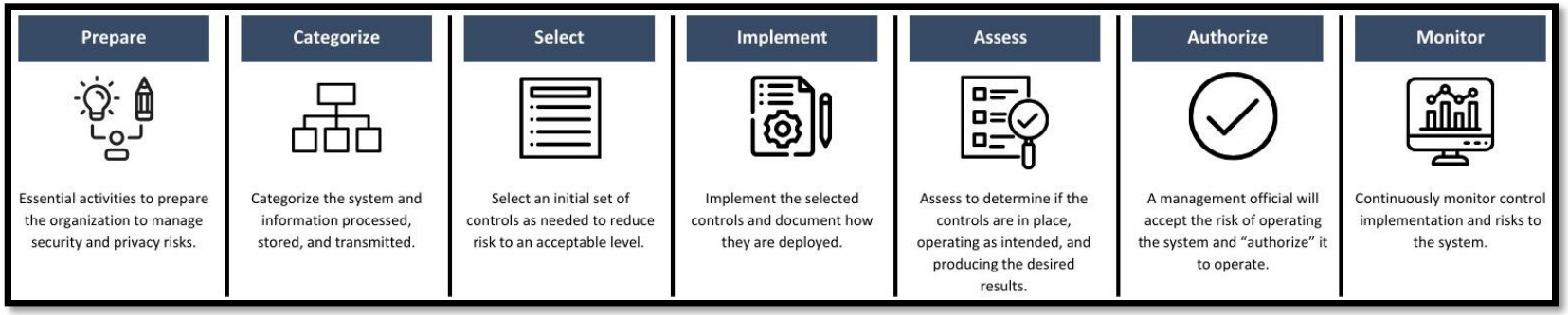
[2] NIST Special Publication (SP) 800-37, Revision 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.

View the full RMF Resource Page

Overview

The Seven Steps of the RMF Process

There are seven steps in the RMF process. All seven steps are required for successful execution of the RMF. The image below lists each step and their respective descriptions. While the process is shown as linear, after initial implementation, organizations can move between steps in any order, as needed.



Tying Organizational Mission to Information Security and Privacy Risk Management

In our current information age, relying on digital capabilities and data processing is essential for achieving organizational missions. This reliance increases potential exposure to information security risks and potential privacy problems for customers, employees, or even society as a whole. A disciplined and structured approach to information security and privacy risk management enables you to understand, for instance:

- What information, technologies, people, processes, etc., are the most critical to your organization's mission?
- What internal or external risks might impede your ability to carry out your mission successfully?
- Who within the organization is accountable for information security and privacy risk management success?
- What steps are needed to minimize or eliminate the possibility of identified risks impeding your mission?

Information Security and Privacy

The RMF addresses both information security and privacy. Though they are distinct disciplines, they can have overlapping and complementary objectives.

For example, when your organization processes personally identifiable information (PII), your information security program and privacy program have a *shared responsibility* for managing the risks to individuals that may arise from unauthorized access to those data. You must keep this in mind when selecting, implementing, assessing, and monitoring appropriate controls. Note, however, protecting individuals' privacy cannot be achieved solely by securing PII.

The risk management processes described in the RMF are equally applicable to security and privacy programs. Learn more about this in section 2.3 of the RMF.

[View the full RMF Resource Page]

Prepare

Getting Started

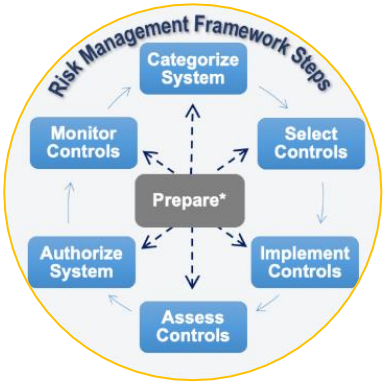
Beginning here, this guide will highlight foundational concepts, tasks, questions, and resources for each step of the RMF. This is not intended to be a comprehensive review of the RMF; it is intended to be introductory. View the full Risk Management Framework for a thorough review of each step.

Getting Started Begins with the Prepare Step

Beginning with the Prepare Step ensures your organization is ready to execute the RMF process in a practical, efficient, and cost-effective manner to achieve your desired risk management outcomes. **Everyone should start with this step and run through the process sequentially for initial implementation.** However, as you are monitoring the controls, you have the flexibility to return to other steps in whichever order, and as frequently as necessary.

Prepare Step Objectives

- ✓ Facilitate better communication between leadership and system owners and operators.
- ✓ Reduce the organization's information technology (IT) and operational technology (OT) infrastructure complexity.
- ✓ Identify, prioritize, and focus resources on the organization's high-value assets that require increased levels of protection.
- ✓ Enable system readiness for implementing the RMF.



Key Terminology*

- **Outcomes:** Cybersecurity and privacy results you hope to achieve through implementation of tasks.
- **Controls**: The countermeasures used to protect the confidentiality, integrity, and availability of a system and its information, or manage privacy risks.
- **Risk Management Strategy:** Strategy that addresses risk tolerance and how organizations intend to assess risk, respond to risk, and monitor risk.

**Definitions provided are intended as plain language. Review the NIST Glossary for official NIST definitions.*

View the full RMF Resource Page

Prepare

Essential activities to PREPARE the organization to manage security and privacy risks.

Foundational Tasks for the Prepare Step

- **Designate an individual, or individuals, who will be assigned the task of executing the Risk Management Framework.** (*Task P-1*)
  Note: Roles and responsibilities may be assigned to personnel internal or external to your organization.

- **Create a risk management strategy for the organization that articulates your organizational risk tolerance.** (*Task P-2*)
  Note: See the next page for more on risk tolerance.

- **Implement a continuous monitoring strategy for your organization to monitor security and privacy risk posture.** (*Task P-7*)
  Note: The strategy articulates frequency of control monitoring and how monitoring is to be conducted.

- **Determine the scope of protection for the system and what falls into that scope.** (*Task P-11*)
  Note: See the next page for more on authorization boundaries.

- **Regularly assess the security and privacy risks at the organization level and system level. Update risk assessment results on an on-going basis.** (*Tasks P-3, P-14*)

Key Terminology*

- **Authorization Boundary:** Components of a system to be authorized for operation, essentially the scope of the "system" for RMF implementation. Sometimes referred to as "system boundary" as well.
- **Risk Tolerance:** Level of risk an organization is willing to assume to achieve a potential desired result.
- **Risk Assessment:** Process of identifying risks to operations assets, individuals, and other organizations resulting from the operation of a system.
- **System:** Combination of interacting elements (such as people, processes, technologies, facilities) organized to achieve one or more stated purposes.

**Definitions provided are intended as plain language. Review the NIST Glossary for official NIST definitions.*

Questions to Consider

- How can we better facilitate communication on cybersecurity and privacy risk management to ensure security and privacy requirements are satisfied, concerns and issues are addressed quickly, and risk management processes are carried out effectively?
- As we prepare to implement a risk management strategy, what expertise do we need to help us achieve our goals?
- What are the highest-value assets we should prioritize protecting?

Related Resources

- RMF Introductory Course
- Prepare Step Frequently Asked Questions

View the full RMF Resource Page

Prepare

Getting Started: Risk Management Strategy and Risk Tolerance

A risk management strategy guides and informs risk decisions – including how risk is **framed, assessed, responded to, and monitored** – making the risk perceptions used in making investment and operational decisions explicit. It helps you:

- **Understand and document** specific assumptions, constraints, risk tolerances, priorities, and trade-offs.
- **Make strategic-level decisions** on how to manage cybersecurity and privacy risk.
- **Define risk tolerance –** the level of risk or degree of uncertainty acceptable to the organization.
  Note: There is no "correct level" of risk tolerance. The degree of risk tolerance is generally based on organizational culture, could be different for different types of losses or compromises, and can be influenced by risk tolerance of executives.

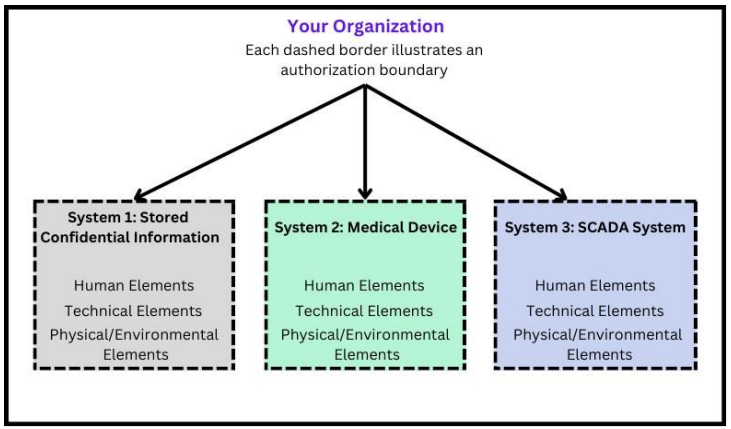
  ***Example:** A higher risk tolerance may mean only addressing specific threats that have impacted peers or competitors. Conversely, a lower risk tolerance may require you to address additional threats—meaning you might have to select more (or different) controls to manage risk.*

Related resources: NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*.

Understanding Authorization Boundaries

The first task is to understand the system, or systems, you are attempting to protect. A system, as defined on the previous page, is the "combination of interacting elements organized to achieve one or more stated purposes." For instance, a system might be an internet-connected medical device, which operates in a particular environment, has human interaction, and is a piece of technical machinery. Or, the system might be a process for handling confidential information—you have a location where you store data; humans who create, modify, store, and transmit data; and authentication processes to access data. Organizations are made up of multiple systems with different functions and types of information, and each requires different safeguards for protection.

When you create an authorization boundary, you draw an imaginary line around the system. Now, you have something you can categorize the risks for and can identify appropriate controls for protecting the system. Similarly, contracts with vendors will need to document authorization boundaries and accountability. What is the scope of *their* responsibility for protecting assets?



Authorization boundaries establish the scope of systems to be protected, managed, and authorized for operation or use.

View the full RMF Resource Page

Categorize and Select

***CATEGORIZE** the system and information processed, stored, and transmitted, then **SELECT** an initial set of controls, or safeguards, to protect the confidentiality, integrity, and availability of your organization's people, systems, and assets.*

Foundational Tasks for the Categorize and Select Steps

- **Once you have identified your most important assets, processes, and systems, categorize each system based on the impact to the organization if the confidentiality, availability, or integrity were to become compromised.** (*Task C-2*)
  Note: See the next page for a sample planning table.

- **Now that you have categorized the systems and assets, select the appropriate controls needed for protection.** (*Task S-1*)
  Examples: Restricting access to specific information types; cybersecurity and privacy literacy & awareness training; data encryption. See NIST SP 800-53 for a catalog of security and privacy controls.

- **After selecting an appropriate control baseline, tailor the controls to address the specific security and privacy requirements for the organization.** (*Task S-2*)
  Note: Organizations use risk assessments to guide the tailoring process. Selected and tailored controls (from Tasks S-1 and S-2) are documented in a security and/or privacy plan.

- **Develop and implement a system-level strategy for monitoring control effectiveness.** (Task S-5)
  Note: This strategy defines how changes to the system and environment of operation are to be monitored, how risk assessments are conducted, and the reporting requirements.

Key Terminology*

- **Control Baseline:** A set of controls you can implement to meet strategic, legal, regulatory, or contractual security and privacy requirements and manage risk.

- **Tailoring:** The process by which security and privacy control baselines are modified to meet your unique risks and needs.

**Definitions provided are intended as plain language. Review the NIST Glossary for official NIST definitions.*

Questions to Consider

- What security and privacy controls are needed to satisfy the organization's security and privacy requirements and to adequately manage risk?
- For our initial selection of controls, should we use a baseline (pre-defined) control selection approach, or should we select our own controls?
- How effective are the controls we have implemented? What is the frequency in which the controls are monitored?

Related Resources

- Security and Privacy Controls Introductory Course
- Control Baselines Introductory Course
- Categorize Step Frequently Asked Questions
- Control Baselines for Information Systems and Organizations

View the full RMF Resource Page

Sample Planning Table for Categorization

You can use this sample planning table to help you begin to identify your most important assets, processes, and systems, and then categorize each system based on the impact to the organization if the confidentiality, availability, or integrity were to become compromised. The italicized text below is provided to illustrate examples. To learn more, NIST Special Publication 800-60, Vol.1, Rev. 1 provides basic guidelines for mapping types of information and information systems to security categories.

System Name: *Stored Administrative Information** **Overall System Impact:** *Moderate*

Information Type	Confidentiality Impact (low, moderate, high)	Integrity Impact (low, moderate, high)	Availability Impact (low, moderate, high)	Notes
Accounting	*Low*	*Moderate*	*Low*	
Payments	*Low*	*Moderate*	*Low*	
Human Resource Strategy	*Low*	*Low*	*Low*	
Employee Performance Management	*Low*	*Low*	*Low*	

**Examples taken from NIST SP 800-60, Vol.2, Rev.1*

System Name: *SCADA (supervisory control and data acquisition) system*** **Overall System Impact:** *High*

Information Type	Confidentiality Impact (low, moderate, high)	Integrity Impact (low, moderate, high)	Availability Impact (low, moderate, high)	Notes
Sensor Data	*N/A*	*High*	*High*	
Non-privacy-related administrative data	*Low*	*Low*	*Low*	

***Examples taken from FIPS Publication 199*

- **Low Impact:** limited adverse effect on organizational operations, assets, or individuals.
- **Moderate Impact:** Serious adverse effect on organizational operations, assets, or individuals.
- **High Impact:** Severe or catastrophic adverse effect on organizational operations, assets or individuals.
- **Overall System Impact:** The level assigned matches the highest level (low, moderate, or high) for confidentiality, integrity, or availability of information on the system; also known as the "high-water mark."

- **Availability:** Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]
- **Confidentiality:** Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]
- **Integrity:** Guarding against improper information modification or destruction. [44 U.S.C., SEC. 3542]

View the full RMF Resource Page

Implement and Assess

***IMPLEMENT* and document the selected controls, then *ASSESS* if the controls selected are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system and the organization.**

Foundational Tasks for the Implement and Assess Steps

- **Now that you have categorized systems by their risks and have selected appropriate controls, now is the time to implement the controls.** (*Task I-1*)
- **Update security and privacy plans to document necessary changes.** (*Task I-2*)
  Note: It's not always feasible to implement controls as planned. Document necessary revisions that reflect how the control is implemented. See NIST SP 800-18 for more guidance.
- **Select an individual or team responsible for conducting a control assessment.** (*Task A-1*)
  Note: Organizations can conduct self-assessments of controls or obtain the services of an independent assessor.
- **Develop, review, and approve plans to assess implemented controls.** (*Task A-2).*
- **Once plans are approved, conduct control assessments using the assessment plans.** (*Task A-3*)
  Note: NIST SP 800-53A provides an assessment methodology and assessment procedures for the security & privacy controls.
- **Prepare an assessment report documenting the findings and recommendations, such as plans for correcting deficiencies.** (*Task A-4*)
- **Prepare the plan of action and milestones, which details remediation plans based on the findings and recommendations of the assessment report.** (*Task A-6*)

Key Terminology*

- **Control Assessor:** The individual, group, or organization responsible for conducting a control assessment.
- **Plan of Action and Milestones:** A document that identifies tasks that need to be accomplished. It details resources required to accomplish the elements of the plan, milestones for meeting the tasks, and the scheduled completion dates for the milestones.

**Definitions provided are intended as plain language. Review the NIST Glossary for official NIST definitions.*

Questions to Consider

- Have the security and privacy controls been implemented or is there an implementation plan in place?
- What is the desired or required level of assurance (i.e., confidence) that the selected controls, as implemented, are effective?
- If you have controls required (such as through contracts, agreements, regulations, or supply chain agreements) by an external party, what are their assessment requirements and procedures?

Related Resources

- Control Baselines Introductory Course
- Implement Step Frequently Asked Questions
- Assessing Security and Privacy Controls Introductory Course

View the full RMF Resource Page

Authorize and Monitor

A senior organization official determines if security and privacy risk based on operation of the system is acceptable, and if so, AUTHORIZES the system. MONITOR the security and privacy posture of the system and organization.

Foundational Tasks for the Authorize and Monitor Steps

- **Assemble the authorization package and submit it to the authorizing official for an authorization decision.** (*Task R-1*)
  Note: If security and privacy controls are being implemented by an external provider, ensure the provider makes available the information needed for your organization to make risk-based decisions.

- **The authorizing official analyzes the information in the authorization package and finalizes the determination of risk to the organization.** (*Task R-2*)

- **The authorizing official issues an authorization decision for the information system, indicating whether the system is authorized to operate or not.** (*Task R-4*)

- **Monitor the system and environment of operation for changes that impact security and privacy.** (*Task M-1*). This can include assessing controls on an ongoing basis based on the continuous monitoring strategy. *(Task M-2)*
  Examples: hardware/software upgrades, changes in personnel, changes in facility location, adversarial attacks, etc.

- **Using the results of the ongoing monitoring activities, risk assessments, and outstanding items in plans of action and milestones, determine the appropriate risk response and implement.** (*Task M-3*)

- **Maintain ongoing communication with organizational leadership to convey the current security and privacy posture of the organization.** (*Task M-5*)

Key Terminology*

- **Authorizing Official:** A senior executive with the authority to authorize (i.e., assume responsibility for) the operation of an information system or the use of a designated set of controls at an acceptable level of risk.
- **Authorization Package:** Authorization packages include:
  - Security and privacy plans
  - Security and privacy assessment reports
  - Plans of action and milestones
  - An executive summary (optional)
- **Continuous Monitoring Strategy:** Strategy to implement continuous monitoring programs that includes metrics to be monitored, monitoring and assessment frequencies, analysis and response actions, and reporting requirements.

**Definitions provided are intended as plain language. Review the NIST Glossary for official NIST definitions.*

Questions to Consider

- Should we invest in a commercially-available governance, risk, and compliance tool to automate how we prepare, assemble, track, and share our security and privacy implementation information?
- Do our reporting procedures provide leadership the information they need about the organization's top cybersecurity and privacy risks and how they're being managed?

Related Resources

- Authorize Step Frequently Asked Questions
- Monitor Step Frequently Asked Questions

View the full RMF Resource Page

View the Full Risk Management Framework

This guide is an introduction to the RMF. View the full RMF and its suite of resources.

Questions?

Email: sec-cert@nist.gov

Additional Resources

- RMF Online Introductory Courses
- RMF Frequently Asked Questions
- Suite of NIST standards and guidelines to support implementation of the RMF
- NIST Small Business Cybersecurity Corner

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE